U.S. ARMY PUBLIC AFFAIRS NEWS RELEASE

Army on Track With Y2K Bug

SGT. 1ST CLASS CONNIE E. DICKEY

WASHINGTON — With 90 percent of both nonmission and mission-critical systems Y2K-compliant, Army officials are confident the millennium bug will not give them any major problems come Jan. 1, 2000.

"We have only a small number of systems yet to become Y2K-compliant, and most of them will be completed by September. Overall, the Army is on schedule," said Miriam Browning, Director of Information Management in the Office of the Director for Information Systems for C4 (Command, Control, Communications and Computers).

She emphasized that included active Army, National Guard, and Reserve. "We will be monitoring the remaining systems closely," but she said, "soldiers should be confident that their weapon systems and computers will work as designed in the year 2000."

In addition, Browning said the computers operated by Defense Finance and Accounting Service have been certified Y2K-compliant, so soldiers, civilians, and contractors need not worry — their checks will be there after Dec. 31.

The Department of the Army has been working the Y2K issue since 1996, Browning said, and developed a DA Y2K Action Plan, which breaks down the approach to the Y2K problem into five phases: awareness, assessment, renovation, validation, and implementation. Most Army systems have completed the implementation phase and are participating in an additional series of integration tests with the Joint CINCs and across Department of Defense functional areas such as finance, personnel, logistics, intelligence, communications, and medical. The purpose of these integration tests is to assure Army systems can operate with other Army and DoD systems successfully in a Y2K environment, Browning said.

Operation Order 99-01 (Millennium Passage) is the Army's Y2K strategic test plan. It outlines the operational threads, systems, and communications equipment to be tested at division, corps, and separate brigades. Army Y2K tests have been conducted at Forts Bliss, Bragg, Drum, and Hood on major tactical systems. Y2K tests at remaining units will be conducted throughout the spring and summer. Army units will be participating in upcoming Y2K test events in Europe and Korea.

Test results to date have been positive, Browning said, with no known instances of any major Y2K or operational failures. Minor incidents such as finding out that a vendor's supposedly Y2K-compliant equipment or software is not Y2K-compliant can usually be fixed within a reasonable amount of time. "Testing is a Y2K real risk reducer," Browning said.

The Y2K problem exists because of the widespread practice of using the last two digits of a year in computer databases, software applications, and hardware chips. If not fixed, com-

RELEASED April 12, 1999

puters will not recognize 00 as 2000, but instead will either read the date as 1900 or fail to respond.

Browning said hardware fixes are easier to handle because typically new chips or computers can simply be bought to replace older ones. Software fixes are a bit more complicated because they involve more date incidences to fix and the production of tailored software coding. Embedded microprocessors are also being reviewed for replacement or software fixes, she said. These embedded chips are found in weapon systems and on installation facility devices such as intrusion detection systems for ammunition storage areas.

In addition to systems' Y2K compliance, installation Y2K readiness is also on the Army's critical path for Y2K. Browning said that each major command has Y2K review teams that have visited installation sites to assure Y2K compliance. "The results are very good overall. Most facility infrastructures such as security, safety, and mission systems are fixed, and the remaining ones should be completed by June 1999."

As a worst-case scenario, the Army also has in place contingency plans to minimize Y2K impacts and disruptions. There are two types of contingency plans. The first are system contingency plans and are required for every Army system. They take into account actions and procedures to use should the system not work. The second type are operational contingency plans. These are connected to the Army's Continuity of Operations Plans and assure that Y2K is covered as part of a unit's mission contingency plans.

Browning said installations also have a requirement to put in place contingency plans. The Fort Eustis, Va., contingency plan is being used as a model for other Army installations.

In the process of fixing Y2K at their installations, commanders are encouraged, Browning said, to outreach to their local communities and work with them on helping to fix Y2K problems. She said a recent message from the Deputy Secretary of Defense issued general priorities for DoD Y2K support to civil authorities.

Browning summarized the Y2K situation. "The Army is in good shape regarding Y2K. However, it is the responsibility of all of us in the Army, especially leaders, to make sure Y2K bugs are uncovered and fixed. If in doubt, ask and fix. It is easier to do this today than January 1, 2000. Our warfighting mission cannot be compromised."

More information on Y2K can be found at several Web sites:

- **http://www.army.mil/army-y2k/Home.html**
- **http://www.hqda.army.mil/acsimweb/ops/y2k.htm**
- **http://www.y2k.gov.**

Editor's Note: This information is in the public domain at **http://www.dtic.mil/armylink/news** on the World Wide Web.